

[Cryptography] keys, signatures, trust, identification, badges, et cetera

ianG [iang at iang.org](mailto:iang@iang.org)

Fri Sep 12 13:20:31 EDT 2014

- Previous message: [\[Cryptography\] keys, signatures, trust, identification, badges, et cetera](#)
- Next message: [\[Cryptography\] distributing fingerprints etc. via QR codes etc.](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

On 10/09/2014 21:27 pm, John Denker wrote:

> On 09/09/2014 09:09 AM, ianG wrote:

>

>> Keysigning parties struggle to make meaning of the signature and of the
>> key. What does it mean when I sign your key?

>

> Indeed! That's the crucial question.

>

> AFAICT the question is unanswerable within PGP's conceptual
> framework, because the framework is too unsophisticated and
> inflexible.

To put it bluntly, PGP community eschews getting too close to the PKI
concept of a CPS, which is supposed to [0] answer this question.

>> In some groups it means

>> "I saw this person" and in others it means "this person's ID matched
>> their key ID text fields."

>

> Indeed! AFAICT the whole idea behind the usual key-signing
> party is predicated on confusing the concepts of identification
> and trust ... which IMHO ought to be kept well separate.

I think there is some merit in confusing the formal channels of
identification. If I meet some dude at a hacker event, I'm more
interested in who he is than that he has some document from some
overbearing state that tries to compress his personality into a 9 digit
string.

> On top of that, the PGP notion of "trust" is far too
> simple to be useful.

Yes. But at least it's benign, unlike some other uses of the term.

> In the real world, I sign /documents/ where the body of
> the document spells out what my signature means in that
> particular context. On another document, my signature
> might mean something else entirely.

>

> You can use PGP to sign documents, which is fine ...
> but in contrast, the idea of a "keys signing keys" is
> inherently ridiculous. There is no way to assign a
> reasonable semantics.

Well, the fundamental flaw is the digital signature as human signing
token. If we could crack doing RSA in the brain then it is possible
we'd be able to make statements here, but all designs end up with
"computer executes code which makes multiplication over hash over
document ..." which is unfortunately too far removed from "user performs
ceremony widely agreed to be local assent."

> In the real world trust is highly multi-dimensional. I
> might trust you with one set of things but not another.

>

> Possibly-constructive suggestion: In the social-media
> world we have /badges/. The more formal name for
> such things is /credentials/. A related concept
> is /certificates/, if we use the word in its broad
> vernacular sense, *not* limiting it to x509 certificates.

[Cryptography] keys, signatures, trust, identification, badges, et cetera

> Examples include driver's licenses, teaching certificates,
> workplace ID badges, et cetera.

This is heading in the right direction, but again I wonder about capturing information in a technical sense without the asserting the providence or pedigree of it. A perhaps powerful example of this idiocy is LinkedIn's endorsements which because they have no foundation end up being noise.

> These serve to split the difference between the highly
> detailed notion of a signed document and the highly
> non-detailed notion of "trust" versus "non-trust" as
> conceived by PGP.
>
> For example, so-and-so might earn a Cryptography List
> badge, which we define to mean that they are a known,
> established contributor to this list. It does *not*
> mean that we have identified the person in any physical
> sense; the contributor could be a sock puppet controlled
> by some unknown person ... or could be the proverbial
> dog typing at the keyboard. The badge -- securely
> associated with a particular PGP public key -- serves
> only to indicate that a message comes from the same
> person (or dog) as last time. This usefully solves a
> /subset/ of the general identification problem, and
> a /subset/ of the general trust problem.

Right, at this level, mere technical solutions that indicate such trivial facts can then be assembled into something that might enter in to a decision to trust. There is a current wave of startups that are analysing social media data in order to assess whether you are a good risk for a loan. As long as they don't go too far, this kind of works, but the danger and inevitability is that they will go too far on reliance on this metric base.

> In general, people rely far too much on credentials.
> A credential is just a symbol. Never confuse a symbol
> with the thing symbolized. However, my main point
> remains: For every problem that credentials have,
> the PGP "trust" model has the same problem only
> orders of magnitude worse.
>
> All this is discussed in more detail, along with some
> related issues, at
> <https://www.av8n.com/security/trust-auth.htm>
>
> I have no idea how hard it would be to create a
> PGP-like system that supports badges.

It wouldn't be that hard, but one of the flaws in the sense of meaning is the absence of any real-world implication of the statement. Typically we would consider things like contracts for legal clout, escrow or insurance for backup, and/or reputation for soft issues.

If trust is on the table, there has to be skin in the game, to use the Americanism. About the only thing possible in the PGP world is reputation as skin, which isn't that much, and not enough to support more than mailing-list or academic contributions. To go further, or to do it properly, something like CAcert's arrangement is needed.

> On 09/08/2014 07:05 PM, Tony Arcieri wrote:
>
>> The main use case I'd like to see is sharing fingerprints (or keys)
>> phone-to-phone.
>
> There's an app for that.
>
>> I recently went to a "keysigning party" (not expecting
>> much) and left with a ton of paperwork to do, and I hate paperwork.
>
> I have not carefully researched the issue, but the
> android app "APG" seems to work fine for that. It can
> put a QR-encoded fingerprint on the screen for others
> to scan, and it can scan QR codes from others and
> interpret them correctly. Details on this and other
> options are discussed at

> <https://www.av8n.com/computer/htm/distributing-keys.htm>

So, exchanging QR codes is just an optimisation of the old fingerprint convention. It improves the tech, the reliability and speed of the old method, but it changes nothing in the semantics.

Life has moved on. What seemed clear and useful in the 1990s is now out of date. The gold standard today is how social networks do it. Which in short is a photo of the person, plus various shared relationships.

I suppose that we should say that those early efforts to put photos inside OpenPGP keys were on the right track, although they didn't really take off in any sense. The question today is how to get that photo across efficiently and reliably, which will typically dominate things like QRs, as we need $o(100)$ times the data and complexity.

iang

[0] But does not typically.

-
- Previous message: [\[Cryptography\] keys, signatures, trust, identification, badges, et cetera](#)
 - Next message: [\[Cryptography\] distributing fingerprints etc. via QR codes etc.](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)
-

[More information about the cryptography mailing list](#)